**PCT** WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06K 19/06 | A1

(11) International Publication Number: WO 00/25262

(43) International Publication Date: 4 May 2000 (04.05.00)

(21) International Application Number: PCT/US99/25423

(22) International Filing Date: 28 October 1999 (28.10.99)

(30) Priority Data:
09/181,734 28 October 1998 (28.10.98) US

(71) Applicant: AMERICAN EXPRESS TRAVEL RELATED SERVICES COMPANY, INC. [US/US]; American Express Tower, World Financial Center, New York, NY 10285 (US).

(72) Inventors: HACKETT, Ann; 15263 South 24th Street, Phoenix, AZ 85048 (US). ARNOLD, Lisa; Building 10400, 10030 North 25th Avenue, Phoenix, AZ 85020 (US). JORDAN, Vickie; 4722 North 53rd Street, Phoenix, AZ 85018 (US).

(74) Agent: SOBELMAN, Howard, L; Snell & Wilmer, L.L.P., One Arizona Center, 400 East Van Buren, Phoenix, AZ 85004-0001 (US).

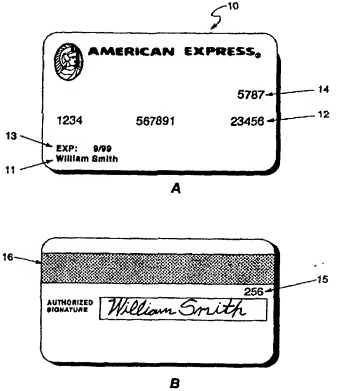
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

**Published**
*With international search report.*

(54) Title: SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION CARD

(57) Abstract

Instead of a PIN which is associated with an account and provides access to an account, a card identification code (14), which is located on the card (10) but does not provide automatic access to an account, is used to verify that the consumer currently possesses the transaction card (10) at the time of purchase and/or is the true card owner. At the time of card printing, an embossing file of account codes (12) including associated identification codes is created and loaded into the account database. At the time of authorization, the identification code (14) and the account code (12) are entered into a POS device and sent to an authorization system. If the identification codes match, and other authorization parameters are satisfied, the transaction card is authorized.



*FOR THE PURPOSES OF INFORMATION ONLY*

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| AL | Albania | ES | Spain | LS | Lesotho | SI | Slovenia |
| AM | Armenia | FI | Finland | LT | Lithuania | SK | Slovakia |
| AT | Austria | FR | France | LU | Luxembourg | SN | Senegal |
| AU | Australia | GA | Gabon | LV | Latvia | SZ | Swaziland |
| AZ | Azerbaijan | GB | United Kingdom | MC | Monaco | TD | Chad |
| BA | Bosnia and Herzegovina | GE | Georgia | MD | Republic of Moldova | TG | Togo |
| BB | Barbados | GH | Ghana | MG | Madagascar | TJ | Tajikistan |
| BE | Belgium | GN | Guinea | MK | The former Yugoslav Republic of Macedonia | TM | Turkmenistan |
| BF | Burkina Faso | GR | Greece | | | TR | Turkey |
| BG | Bulgaria | HU | Hungary | ML | Mali | TT | Trinidad and Tobago |
| BJ | Benin | IE | Ireland | MN | Mongolia | UA | Ukraine |
| BR | Brazil | IL | Israel | MR | Mauritania | UG | Uganda |
| BY | Belarus | IS | Iceland | MW | Malawi | US | United States of America |
| CA | Canada | IT | Italy | MX | Mexico | UZ | Uzbekistan |
| CF | Central African Republic | JP | Japan | NE | Niger | VN | Viet Nam |
| CG | Congo | KE | Kenya | NL | Netherlands | YU | Yugoslavia |
| CH | Switzerland | KG | Kyrgyzstan | NO | Norway | ZW | Zimbabwe |
| CI | Côte d'Ivoire | KP | Democratic People's Republic of Korea | NZ | New Zealand | | |
| CM | Cameroon | | | PL | Poland | | |
| CN | China | KR | Republic of Korea | PT | Portugal | | |
| CU | Cuba | KZ | Kazakstan | RO | Romania | | |
| CZ | Czech Republic | LC | Saint Lucia | RU | Russian Federation | | |
| DE | Germany | LI | Liechtenstein | SD | Sudan | | |
| DK | Denmark | LK | Sri Lanka | SE | Sweden | | |
| EE | Estonia | LR | Liberia | SG | Singapore | | |

# SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION CARD

## BACKGROUND OF THE INVENTION

1. Technical Field

The present invention relates, generally, to transaction card fraud reduction systems and methods and, more particularly, to verifying that a consumer is in possession of a transaction card and/or is the true card owner during a purchase transaction.

2. Background Information

Transaction cards such as, for example, credit cards, debit cards, bank cards, charge cards, smart cards and the like, have become increasingly popular for purchasing goods and services and for conducting other transactions. A transaction card typically includes information related to the issuer's name and logo, an account number, an expiration date and the cardholder's name. The cards may also have other information, serial number and/or the like printed on the card to represent other information about the transaction card or about the card member such as, for example, a group number, a promotion number, a card type number, a plastic issuance number and/or the like. Certain information is often embossed on the card with raised print, thereby allowing the information to be imprinted on a charge slip; however, the information that is unembossed (flat) would not be imprinted onto the charge slip. For many transaction cards, the information printed on the card is also contained within a magnetic stripe, a bar code and/or an integrated circuit (microchip) for automatic downloading/reading by a card reader.

Many card transactions are commenced by inserting, or sliding a card through, a card reader which automatically downloads the card information, thereby allowing the information to be used during the authorization process without the need for manual input or review of the card information. However, because of the substantial increase in fraudulent use and theft of transaction cards, the use of the card information is often supplemented by various fraud prevention techniques, such as requiring a signature to verify the consumer's agreement to the transaction or the entry of a PIN number to verify the consumer's authority to use the transaction card. Additionally, certain card issuers,

such as banks, incorporate the consumer's picture onto the face of the transaction card to give the merchant an additional verification procedure.

While the use of a signature, PIN or picture is effective for fraud reduction when the cardholder presents a card to a merchant, these options are not as effective, and may not be available, for other transactions. Particularly, transactions which do not require face-to-face contact between a consumer and merchant, such as the use of a transaction card to purchase items through the Internet or over the telephone (e.g., mail order). Moreover, many transactions may be alternatively completed without using the physical transaction card. For example, a consumer or merchant may simply key in the transaction card number into the keypad of a POS device or the keypad on an ATM.

When conducting Internet, telephone or keypad transactions, a cardholder may only need to provide a card account number and expiration date to allow the merchant to charge a particular account and verify that the transaction card is valid. Other verification information, such as a PIN number, is usually not disclosed because the PIN is typically memorized by the cardholder and never disclosed to anyone. Because merchants often only request limited information to conduct a transaction over the Internet or the telephone, an increased potential for fraud exists due to the increased availability of this general information. In other words, regardless of a consumer's possession of the physical transaction card, a consumer can still fraudulently obtain and provide this general information.

Particularly, cardholders often provide a transaction card number to telemarketers, merchants, bank tellers and Internet sites, thereby allowing a merchant or clerk to retain the credit card number and associated information for later fraudulent use. Moreover, a person may overhear a transaction card number being disclosed over the telephone or, with the increase of mailbox thefts, a person may obtain a credit card number from a billing statement or promotional literature. Furthermore, advanced computer operators are able to intercept transaction card numbers which are transmitted over modems and/or the Internet. Accordingly, when a merchant simply requests a credit card number from a consumer, it is difficult for the merchant to ensure that the consumer placing the order has the transaction card in his or her possession and/or is the true cardmember, rather than using a stolen account number.

As stated above, the use of PIN numbers are typically limited to face-to-face or ATM transactions wherein the consumer personally enters a PIN into a keypad and the merchant does not need to have knowledge of the PIN. In non face-to-face transactions, the PIN would need to be disclosed to the merchant. However, due to security concerns, consumers prefer to not disclose their private PIN number to merchants and especially prefer to not disclose the PIN number over a telephone or through the Internet. Particularly, a PIN number is directly associated with the account number, and as such, may provide increased access to a transaction card account during a fraudulent transaction. Accordingly, a system is needed which allows the consumer to disclose a security number which is associated with the account number, but does not allow automatic access to the account.

## BRIEF SUMMARY OF THE INVENTION

Due to security concerns during non face-to-face commercial transactions, consumers prefer to not disclose their private PIN number to merchants and especially prefer to not disclose the PIN numbers over a telephone or through the Internet. Instead of a PIN which is associated with an account and provides access to an account, a card identification code, which is located on the card but does not provide automatic access to an account, is used to verify that the consumer currently possesses the transaction card at the time of purchase and/or is the true card owner.

Along with the account number, a transaction card includes a non-embossed four-digit or three-digit number, called a card identification code. During creation of a transaction card, a five-digit identification code is calculated from the account number, four-digit or three-digit identification code and the expiration date based upon a predetermined algorithm. A four-digit identification code is printed on the front of the card, an associated five-digit identification code is entered into the magnetic stripe and an associated three-digit identification code is printed in the signature panel. An embossing file of account numbers including associated identification codes is created and loaded into the account database. At the time of authorization, the four-digit number on the front of the card and the account number are manually keyed into a POS device and sent to an authorization system. The four-digit number is matched to the four-digit number on file

for that transaction card. If the four-digit numbers match, and other authorization parameters are satisfied, the transaction card is authorized.

Alternatively, when the card is swiped through a POS device, the five-digit number previously entered into the magnetic stripe, along with other information, is automatically transmitted to the authorization system. The five-digit number is decomposed using a mathematical algorithm, and the resulting three-digit and/or four-digit numbers are matched against the database record (which includes the originally assigned three or four-digit identification codes for the account number). If the respective three or four-digit numbers match, and other authorization parameters are satisfied, the transaction card is authorized.

Thus, the entry of an additional identification code helps verify that the consumer currently possesses the transaction card at the time of purchase or is the true card owner, rather than simply using a stolen account number. Accordingly, requiring entry of an identification code along with the account number provides an effective deterrent to fraudulent use of the account number. For example, systems and methods in accordance with the present invention at certain tested locations have provided fraud reduction of approximately 78%.

## BRIEF DESCRIPTION OF SEVERAL VIEWS OF THE DRAWINGS

The subject invention will hereinafter be described in conjunction with the appended drawing figures, wherein like numerals denote like elements, and:

Figure 1 is an exemplary flow diagram of the card creation and identification code creation process;

Figure 2a is a front view of an exemplary transaction card showing an account number and card identification code;

Figure 2b is a rear view of an exemplary transaction card showing magnetic strip and card identification code;

Figure 3 is an exemplary schematic diagram of a simplified transaction card authorization system;

Figure 4 is an exemplary schematic diagram of an authorization database with associated identification codes in accordance with an embodiment of the present invention; and,

Figure 5 is an exemplary flow diagram of the authorization process.

## DETAILED DESCRIPTION OF THE INVENTION

To reduce fraud when conducting commercial transactions (i.e., the purchase of goods and services) using a transaction card 10, the present system requests entry of an additional number to help verify that the consumer has possession of the transaction card at the time of purchase or is the true card owner, rather than simply using a stolen account code. Wherein a PIN number is typically memorized and not written down, the present number, called a card identification code 14, 15 and 16, is preferably printed on or encoded in transaction card 10. Due to security concerns during non face-to-face transactions, consumers prefer to not disclose their private PIN number to merchants and especially prefer to not disclose the PIN number over a telephone or through the Internet. Instead of a PIN which is associated with an account and provides access to an account, a card identification code 14, 15 and 16, which does not provide automatic access to an account, is used to help verify that the consumer currently possesses the transaction card at the time of purchase and/or is the true card owner.

With momentary reference to Figure 2a, in accordance with the present invention, a transaction card 10 includes any device suitably configured to display an account code 12 and a card identification code 14. In a preferred embodiment, the transaction card is a credit card, charge card, debit card, smart card, bank card and/or the like. Transaction card 10 preferably includes information for conducting a transaction. In a preferred embodiment, the front face of transaction card 10 includes an account code 12 and a card identification code 14 located above account code 12. Account code 12 includes any number of characters (n characters) comprising any combination of numbers, letters, symbols or other indicia which are suitably configured to identify a transaction account. In a preferred embodiment, account code 12 is a 15-digit number which identifies an account code, including a routing number or other similar transaction numbers, corresponding to the card owner. One of ordinary skill in the art will appreciate that

account code 12 may be associated with an individual account, a corporate account, an organization account, or any other entity and the account may represent a charge account, a credit account, a debit account, an electronic purse account, or any other financial account.

Card identification codes 14, 15 and 16 include any number of characters (n characters) comprising any combination of numbers, symbols, letters, or other indicia suitably configured to provide verification that the consumer has an actual card in possession at the time of purchase and/or is the true card owner, rather than simply using a stolen account code. In a preferred embodiment, card identification code 14 is printed on or encoded in transaction card 10. Card identification code 14 may be located on either side of the card, encoded into a medium on the card and may be embossed (raised lettering) or unembossed (flat) into the plane of the card. In a particularly preferred embodiment, card identification code 14 is located on the front face of transaction card 10 on the same side as, and above, account code 12. Moreover, card identification code 14 is preferably a four-digit, unembossed (flat) number printed within the plane of the card. One skilled in the art will appreciate that, along with other card member information, card identification codes 14, 15 or 16 may be initially printed on many transaction cards 10 before, during or after account code 12 is printed on transaction card 10. In a preferred embodiment, card identification codes 14 or 15 are logically related to card identification code 16.

After a consumer is approved for a transaction card, an account code 12, a four-digit identification code 14 and/or a three digit code 15, an expiration date 13 and other information are associated with the consumer's name in an account database 30 (see Figures 2a and 3). With reference to Figures 1 and 3, account code 12, a four-digit identification code 14 (or a three-digit identification code 15), an expiration date 13 and other information from account database 30 are preferably transmitted to a card creation system 32 (step 38). In a preferred embodiment, at the time of creating transaction card 10 for the consumer in accordance with the present invention, a five-digit identification code 16 is suitably calculated from account code 12, four-digit identification code 14 or three-digit identification code 15 and expiration date 13 based upon a predetermined algorithm (step 40). Five-digit identification code 16 is preferably calculated and encoded

into the magnetic stripe because five-digit identification code 16 provides additional security by not being disclosed on the face of the card (only four-digit code 14 or three-digit code 15 are visible).

After determining identification codes 14, 15 and 16, transaction card 10 is preferably created with an embossed account code 12, embossed expiration date 13, embossed consumer's name 11 and non-embossed card identification codes 14, 15 and 16 (step 42). Particularly, in a preferred embodiment, a four-digit identification code 14 is printed (non-embossed) on the front of card 10 above account code 12, an associated five-digit identification code 16 is encoded into the magnetic stripe and an associated three-digit identification code 15 is printed in the signature panel. One skilled in the art will appreciate that any one of the aforementioned card identification codes 14, 15 and 16 may exist throughout this process alone or in any combination with the other card identification codes. For example, only identification code 14 may appear on the front of the card without any codes on the back of the card or in the magnetic stripe. Moreover, identification codes 14, 15 and 16 may comprise any number of digits, symbols, characters, letters and/or the like and may be located in any location and in any medium on card 10. For example, an identification code may be encoded into an integrated circuit in a smart card embodiment.

Upon printing of transaction cards 10, an embossing file 34 including card identification codes 14, 15 and 16 is created (step 44). Embossing file 34 with associated identification codes 14, 15 and 16 is next uploaded into account database 30 (step 46). In a preferred embodiment, authorization server 26 communicates with, and analyzes the data within, account database 30 (step 48). Alternatively, the use of a Hardware Security Module allows embossing file 34 to provide a simplified, more direct transmission of embossing information to account database 30 without the need for maintenance uploads. In a particularly preferred embodiment, as shown in Figure 4, identification codes are stored in a look-up table within account database 30.

Referring to Figure 3, an exemplary authorization system 20, account database 30 and card creation system 32 is shown. Authorization system 20 is any authorization system suitably configured to authorize a transaction card and notify an input device 22 of the authorization status. One skilled in the art will appreciate that authorization system

20 can be an existing authorization system, such as the Central Authorization System used by American Express, which is re-programed or re-configured to preform the functions of the present invention or is a system specially configured to preform the functions of the present invention. In a preferred embodiment, authorization system 20 includes input device 22, network 24 and authorization server 26. Input device 22 is any device suitably configured to accept transaction information and transmit the information for approval. In a preferred embodiment, input device 22 is a telephone, computer, point-of-sale terminal, ATM and/or the like. Input device 22 preferably communicates with network 24, wherein network 24 is any device or software suitably configured to transmit information. In a preferred embodiment, network 24 is a modem, a PSTN, an Internet, an Intranet, a direct link, or any combination thereof.

With continued reference to Figure 3, network 24 provides a communication link between input device 22 and authorization server 26. Authorization server 26 is any device suitably configured to authorize a transaction and/or transaction card and notify input device 22 of the authorization status. In a preferred embodiment, authorization server 26 is a centralized authorization system including transaction account codes. One skilled in the art will appreciate that authorization server 26 can be a centralized database providing authorization information to various input devices 22. Moreover, one skilled in the art will appreciate that authorization server 26 may include any combination of components, software, servers and computers suitably configured to not only authorize transactions and/or transaction cards, but also to provide additional transaction support such as report generation and promotional programs. Authorization server 26 is preferably in communication with, and interrogates, account database 30. One skilled in the art will appreciate that account database 30 can be a separate component, integrated into authorization server 26 or simply software within authorization server 26 or within input device 22. In a preferred embodiment, account database 30 includes a look-up table (see Figure 4), thereby allowing verification of the association between account codes 12 and identification codes 14, 15 and 16.

Referring to Figure 5, when a consumer uses transaction card 10, a clerk, sales representative, merchant, consumer or other authorized person inputs account code 12 and card identification code 14, 15 or 16, along with any other transaction information

such as purchase amount, etc., into input device 22 (step 50). In one embodiment, card identification code 14 or 15 is manually keyed into input device 22. The keyed information is sent via network 24 to authorization server 26 (step 51). Authorization server 26 suitably determines if the data was keyed in or swiped through input device 22 (step 52). In a preferred embodiment, to help determine if the data was keyed or swiped, the keyed data includes different formatting, uses different communication lines, different number of digits in the identification code and/or different header information than information read from the magnetic stripe.

After authorization server 26 determines that the information is manually keyed information, authorization server 26 suitably interrogates account database 30 to determine if the keyed identification code 14 or 15 matches the respective identification number on file for that transaction card (step 54). If the respective identification codes 14 or 15 match, the authorization process proceeds to determine if other authorization parameters are satisfied (step 58). If the respective identification codes 14 or 15 do not match, the transaction is denied and an "invalid Card ID" message is transmitted to the input device 22 (step 60). In an alternative embodiment, if the identification numbers do not correspond, authorization server 26 preferably prompts input device 22 to re-enter the card identification code and the process is repeated. If the numbers do not correspond again, transaction card 10 is denied.

When the card is swiped through a POS device 22, the five-digit number previously entered into the magnetic stripe, along with other information, is automatically transmitted to authorization server 26. Authorization server 26 suitably determines that the data originated from a magnetic stripe (step 52) by various methods such as, for example, data format, communication lines from which the data was sent, header information and/or the number of digits in the identification code. Authorization server 26 preferably decomposes the five-digit identification code 16 into a four-digit number using a predetermined mathematical algorithm (step 56). In a preferred embodiment, this algorithm is the inverse of the algorithm set forth above used to create the five-digit identification code 16. Alternatively, account database 30 includes five-digit identification codes 16 for each account code 12, thereby eliminating the need to transform the five-digit code 16 to a four-digit code 14. The algorithm is optimally a robust and secure

algorithm which conforms to the Data Encryption Standard. Similar to above, authorization server 26 then suitably interrogates account database 30 to determine if the derived four-digit number 14 matches the four-digit number on file for that transaction card (step 54). If the four-digit numbers match, the authorization process proceeds to determine if other authorization parameters are satisfied (step 58). If the four-digit numbers do not match, the transaction is denied and an "invalid Card ID" message is transmitted to the input device 22 (step 60). In an alternative embodiment, if the numbers do not correspond, authorization server 26 preferably prompts input device 22 to re-swipe the card identification code 16 and the process is repeated. If the numbers do not correspond again, transaction card 10 is denied.

In a further alternative embodiment, the incorporation of card identification code 14 into a particular authorization process is optional depending on the type of transaction card 10 or account code 12 used for the financial transaction. In other words, when authorizing a transaction, the same authorization system 20 may not require a card identification code 14 for particular account codes 12. For example, certain consumers may be enrolled in a promotional program which includes a cardless account without a card identification code 14. As such, while other verification means typically exist, authorization server 26 may not require entry of an identification code or account database 30 may include any suitable automatic authorization for certain ranges of account codes 12, regardless of entry of a card identification code 14.

In a preferred embodiment, account codes 12 are subject to periodic update as new card promotions or new accounts are opened. For security reasons, card identification codes 14, 15 or 16 are preferably only retained in authorization server 26 until authorization or rejection is received by input device 22. Moreover, in a preferred embodiment, card identification codes 14, 15 or 16 are not permanently stored in the input device 22 or the authorization server 26 and are not printed on documents (i.e., receipts, tickets, itineraries, etc.).

Although the invention has been described herein in conjunction with the appended drawings, those skilled in the art will appreciate that the scope of the invention is not so limited. Modifications in the selection, design and arrangement of various components and steps discussed herein may be made without departing from the scope of the

invention as set forth in the claims. Moreover, the present invention may be described herein in terms of functional block components and various processing steps. It should be appreciated that such functional blocks may be realized by any number of hardware components configured to perform the specified function. For example, the present invention may employ various integrated circuit components, e.g., memory elements, digital signal processing elements, look-up tables, and the like, which may carry out a variety of functions under the control of one or more micro-processors or other control devices.

In addition, those skilled in the art will appreciate that the present invention may be practiced in any number of data communication contacts and that the authorization system described herein is merely one exemplary application for the invention. Further, it should be noted that the present invention may employ any number of conventional techniques for data transmission, training, signal processing and conditioning, and the like. Such general techniques that may be known to those skilled in the art are not described in detail herein.

CLAIMS

1. A system for authorizing commercial transactions comprising:

a transaction card having an n character account code and an n character identification code, wherein said identification code is not an expiration date and wherein said account code and said identification code have a predetermined logical relationship;

an input device for receiving said account code and said identification code; and,

an authorization computer in communication with said input device, said authorization computer configured to confirm said predetermined relationship between said account code and said identification code.

2. The system of claim 1, wherein said transaction card is at least one of a credit card, debit card, bank card, charge card and smart card.

3. The system of claim 1, where in said identification code is unembossed.

4. The system of claim 1, wherein said account code and said identification code are on the same side of said transaction card.

5. The system of claim 1, wherein said input device is at least one of a keypad, POS terminal, ATM terminal, computer and telephone.

6. The system of claim 1, wherein said identification code is at least one of a three-digit number, four-digit number and five-digit number.

7. The system of claim 1, wherein said account code and said identification code are on the same side of said transaction card and said identification code is an unembossed four-digit number located above said account code.

8. The system of claim 1, wherein said authorization computer is configured to transform said identification code to a second identification code.

9. The system of claim 1, wherein said authorization computer communicates with an account database and said authorization computer is configured to confirm said predetermined relationship between said account code and said identification code by interrogation of said account database.

10. A method for authorizing commercial transactions comprising:

keying an n character account code and an n character identification code into an input device, wherein said identification code is not an expiration date and wherein said account code and said identification code have a predetermined logical relationship;

communicating, from said input device to an authorization computer, said account code and said identification code; and,

confirming, at said authorization computer, said predetermined relationship between said account code and said identification code.

11. The method of claim 10, wherein said keying step includes keying said n character account code and said n character identification code into said input device, wherein said input device is at least one of a keypad, POS terminal, ATM terminal, computer and telephone.

12. The method of claim 10, wherein said keying step includes keying said account code and said identification code which are located on a transaction card, further wherein said account code and said identification code are printed on the same side of said transaction card and said identification code is an unembossed four-digit number located above said account code.

13. The method of claim 10, further comprising transforming, via said authorization computer, said identification code to a second identification code.

14. The method of claim 10, further comprising communicating between said authorization computer and an account database and confirming, via said authorization computer, said predetermined relationship between said account code and said identification code by interrogating said account database.

15. A transaction card for authorizing commercial transactions comprising:

an n character account code in a first field;

an n character identification code in a second field, wherein said identification code is not an expiration date;

wherein said account code and said identification code have a predetermined logical relationship;

said transaction card configured to provide, via an input device, said account code and said identification code to an authorization computer, wherein said authorization computer is configured to confirm said predetermined relationship between said account code and said identification code.

16. The system of claim 15, wherein said transaction card is at least one of a credit card, debit card, bank card, charge card and smart card.

17. The system of claim 15, wherein said account code and said identification code are on the same side of said transaction card and said identification code is an unembossed four-digit number located above said account code.

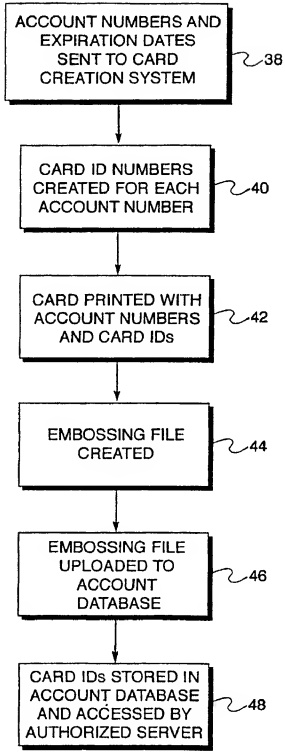

ACCOUNT NUMBERS AND EXPIRATION DATES SENT TO CARD CREATION SYSTEM
38
CARD ID NUMBERS CREATED FOR EACH ACCOUNT NUMBER
40
CARD PRINTED WITH ACCOUNT NUMBERS AND CARD IDs
42
EMBOSSING FILE CREATED
44
EMBOSSING FILE UPLOADED TO ACCOUNT DATABASE
46
CARD IDs STORED IN ACCOUNT DATABASE AND ACCESSED BY AUTHORIZED SERVER
48

*FIG. 1.*

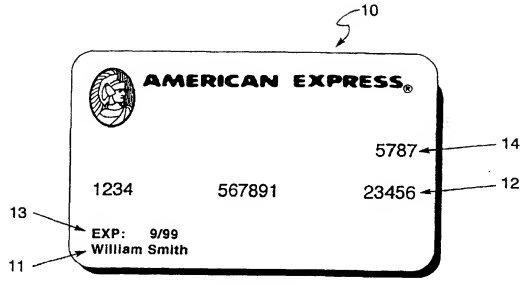

10
AMERICAN EXPRESS®
5787
14
1234
567891
23456
12
13
EXP: 9/99
William Smith
11

FIG. 2A.

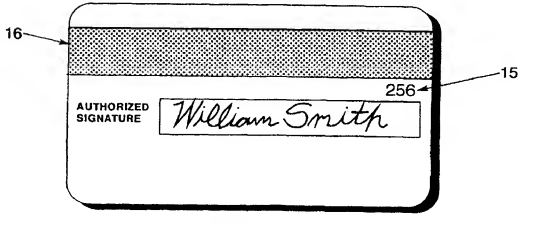

16
256
15
AUTHORIZED SIGNATURE
William Smith

FIG. 2B.

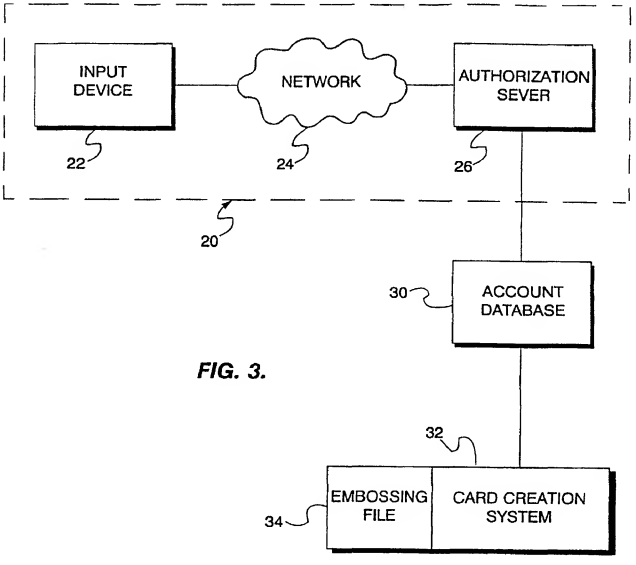

INPUT DEVICE
NETWORK
AUTHORIZATION SEVER
22
24
26
20
30
ACCOUNT DATABASE
32
EMBOSSING FILE
34
CARD CREATION SYSTEM

*FIG. 3.*

| 12 ACCOUNT CODE | 13 EXP. DATE | 14 4-DIGIT ID CODE | 15 3-DIGIT ID CODE | OTHER INFO |
|---|---|---|---|---|
| 1234 567891 11121 | 1/99 | 1765 | 212 | |
| 3141 516178 19202 | 1/00 | 8274 | 314 | |
| 2122 232435 26278 | 5/99 | 5933 | 103 | |
| 3456 789101 12134 | 7/98 | 4116 | 149 | |
| 5678 910112 13145 | 6/99 | 3821 | 586 | |
| 1617 181920 21222 | 5/99 | 9298 | 567 | |
| " | " | " | " | |
| " | " | " | " | |
| " | " | " | " | |
| " | " | " | " | |

30

*FIG. 4.*

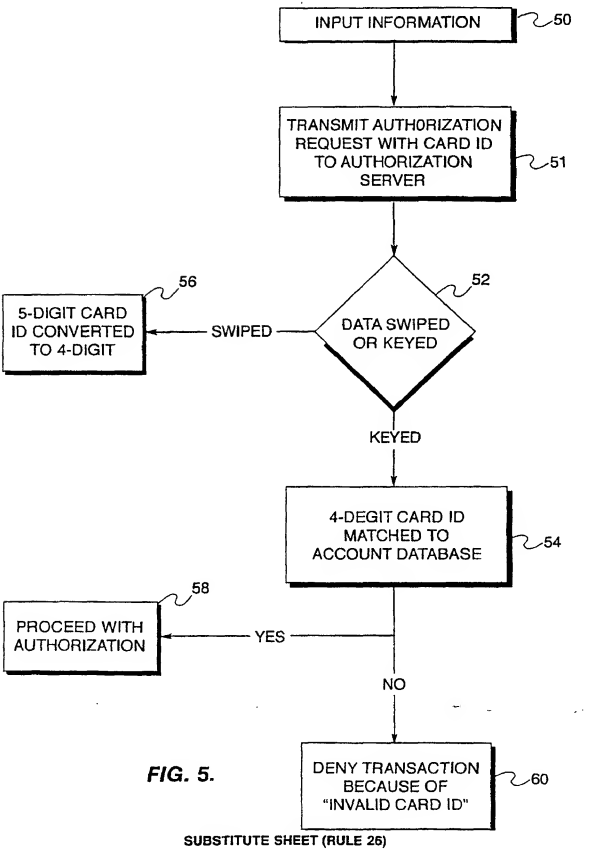

INPUT INFORMATION
50
TRANSMIT AUTHORIZATION REQUEST WITH CARD ID TO AUTHORIZATION SERVER
51
DATA SWIPED OR KEYED
52
SWIPED
5-DIGIT CARD ID CONVERTED TO 4-DIGIT
56
KEYED
4-DEGIT CARD ID MATCHED TO ACCOUNT DATABASE
54
YES
PROCEED WITH AUTHORIZATION
58
NO
DENY TRANSACTION BECAUSE OF "INVALID CARD ID"
60

*FIG. 5.*

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/25423

**A. CLASSIFICATION OF SUBJECT MATTER**

IPC(6) :G06K 19/06
US CL. :235/380, 379, 492, 382.5, 487
According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

U.S. : G06K 19/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

None

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

None

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | US 4,734,568 A (Watanabe) 29 March 1988 (29-03-1988), see the entire reference. | 1-17 |
| Y | US 4,831,245 A (Ogasawara) 16 May 1989 (16-05-1989), see the entire reference. | 1-17 |
| Y | US 5,400,082 A (Kamiya) 21 March 1995 (21-03-1995), see the entire reference. | 1-17 |

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

| | | | |
|---|---|---|---|
| * | Special categories of cited documents: | "T" | later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention |
| "A" | document defining the general state of the art which is not considered to be of particular relevance | "X" | document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone |
| "E" | earlier document published on or after the international filing date | "Y" | document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art |
| "L" | document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) | "&" | document member of the same patent family |
| "O" | document referring to an oral disclosure, use, exhibition or other means | | |
| "P" | document published prior to the international filing date but later than the priority date claimed | | |

| | |
|---|---|
| Date of the actual completion of the international search<br>23 DECEMBER 1999 | Date of mailing of the international search report<br>10 FEB 2000 |
| Name and mailing address of the ISA/US<br>Commissioner of Patents and Trademarks<br>Box PCT<br>Washington, D.C. 20231<br>Facsimile No. (703) 305-3230 | Authorized officer<br>Thien Le<br>Telephone No. (703) 305-3900 |

Form PCT/ISA/210 (second sheet)(July 1992)*